UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,794	01/17/2001 .	Vinay Deo	M61.12-0685	8460

7590 03/25/2004

John A. Wiberg
Westman, Champlin & Kelly
Suite 1600
International Center 900 Second Avenue South
Minneapolis, MN 55402-3319

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	3

DATE MAILED: 03/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/764,794	Applicant(s) DEO ET AL.	
	Examiner Michael J Simitoski	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *37-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *37-44* is/are rejected.

7)☒ Claim(s) *42* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The preliminary amendment of 17 January 2001 has been received.

2. Claims 37-44 are pending.

Claim Objections

3. Claim 42 is objected to because of the following informalities:

a. The word "based" from the second to the last line on page 71 should be replaced with "base".

b. The phrase "wherein the processing component" should be replaced with "wherein the processor component".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 37-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 37 recites the limitation "message specific data derived from the information to be transmitted", but it is unclear whether the data portion includes data specific to the transmission message or only data derived from the information to be transmitted. Claims

38-44 are rejected based on their dependence upon claim 37. *For the purposes of this office action, "message specific data" is understood to mean "transmission message specific data".*

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 37 & 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over "GSM Digital cellular telecommunications system (Phase 2); Security related network functions (GSM 03.20 version 4.4.1)" by ETS in view of U.S. Patent 5,689,563 to Brown et al. (Brown) in view of U.S. Patent 5,343,527 to Moore in further of Applied Cryptography, Second Edition by Schneier.

Regarding claim 37, ETS discloses a mobile station deriving a first encryption key/Kc based on a base key/Ki known by the receiver component/network and a data string/RAND (page 25, Fig. 4.1). ETS lacks a key being based on information specific data. However, Brown teaches that to avoid problems associated with reassembling packets for decryption (col. 3 lines 39-53), one can encrypt packets using an encryption key and a unique pack number as encryption variables (that is unique to each message); the unique pack number and encrypted packet of the message is communicated between the mobile unit and the receiver (col. 7 line 59 – col. 8 line 44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further use message-specific data/unique pack number to create the

encryption key and include the data in the message. One of ordinary skill in the art would have been motivated to perform such a modification to avoid problems associated with reassembling packets for decryption, as taught by Brown (col. 3 lines 39-53 & col. 7 line 59 – col. 8 line 44). As modified, ETS lacks a second encryption key, hashing the message with the first encryption key to obtain a signature, encrypting the signature and message/information with the second key and joining the encrypted message with the message specific data. However, Moore teaches that, to provide an indication that data has been modified, one can hash the data (col. 2 lines 8-13). Moore discloses hashing information to be transmitted/encrypted software to obtain a signature/digest and encrypting the signature/digest, with an encryption key, to obtain an encrypted message (Fig. 3 & col. 2 lines 28-64). Further, Schneier teaches that message authentication codes (keyed hashes) are useful to provide authenticity without secrecy, as only someone with the identical key can verify the hash (page 455 §18.14). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the first key to hash the information to be transmitted and encrypt and to generate a second key to be used to encrypt the message. One of ordinary skill in the art would have been motivated to perform such a modification to provide an indication that data has bee modified, as taught by Moore (Fig. 3 & col. 2 lines 8-13 & lines 28-64) and to allow only someone with an identical key to verify the hash, as taught by Schneier (page 455 §18.14). As modified, ETS discloses communicating the message-specific data/unique pack number to the receiver, but does not explicitly disclose joining the message with the message-specific data/unique pack number in unencrypted form. However, to serve as a means to rejoin the packets of a message, the message-specific data must accompany the message, or ordering would fail.

Regarding claim 44, ETS discloses the mobile device/mobile station storing values/TMSI determining the operation of the mobile device, wherein the mobile device receives a programming message for programming the values into the device (page 25, Fig. 4.1). While ETS does not specifically disclose a radio receiver (as the ETS specifications describe only the interaction between a mobile station/originator and a network/receiver, the physical specifications of the device being variable), the standard disclosed by ETS is a specification for the Digital cellular telecommunications system where mobile phones and other devices of the like (containing radio receivers) interact with a network through cellular communication.

8. Claims 38, 41 & 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over ETS in view of Brown, Moore and Schneier in further view of U.S. Patent 5,701,316 to Alferness et al. (Alferness).

Regarding claims 38 & 41, ETS discloses a system, as modified above, but the originator/mobile station lacks a header generation component and a checksum component. However, Alferness teaches that with increasing traffic across networks, there is a need to perform checksum calculations as a means to detect transmission errors, wherein the checksum is usually inserted into the header information for the message (col. 1 lines 53-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include in the originator/mobile station a checksum component and a header generation component to generate a checksum and insert the checksum in a header. One of ordinary skill in the art would have been motivated to perform such a modification to detect data transmission errors, as taught by Alferness (col. 1 lines 53-67).

Regarding claim 42, ETS discloses a system, as modified above, where a network/receiver generates the same key as a mobile station, based on the same inputs (pages 17 & 25), but lacks specific disclosure of a driver component in the network/receiver deriving the keys from the base key, first and second data strings and the message-specific data; the ETS specifications describe only the interaction between a mobile station/originator and a network/receiver, the physical specifications of the device being variable. However, the key generation and signing process disclosed by ETS and modified by Brown, Moore, Schneier and Alferness above, takes first and second data strings, message-specific data and a base key as it's input. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to instruct the receiver component/network to derive the keys from the base key, first and second data strings and message-specific data to verify the encrypted signature created by originator/mobile station, as is known in decryption art. One of ordinary skill in the art would have been motivated to perform such a modification to provide an indication that data has been modified, as taught by Moore (Fig. 3 & col. 2 lines 8-13 & lines 28-64) and to allow only someone with an identical key to verify the hash, as taught by Schneier (page 455 §18.14).

Regarding claim 43, ETS discloses a system, as modified above, but lacks the receiver/network having a driver component wherein the driver component further comprises a validation component configured to calculate a checksum and compare the calculated checksum to determine whether the message is valid. However, Alferness teaches that with increasing traffic across networks, there is a need to perform checksum calculations as a means to detect transmission errors, wherein the checksum is usually inserted into the header information for the

message (col. 1 lines 53-67) and verified by the receiver comparing the generated checksum with a newly calculated checksum (col. 2 lines 1-16). If the two are equivalent, then no errors are present (col. 2 lines 1-16). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include in the originator/mobile station a checksum component and a header generation component to generate a checksum and insert the checksum in a header. One of ordinary skill in the art would have been motivated to perform such a modification to detect data transmission errors, as taught by Alferness (col. 1 lines 53-67 & col. 2 lines 1-16).

9. Claims 39 & 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over ETS in view of Brown, Moore and Schneier in further view of U.S. Patent 6,049,018 to Hardy et al. (Hardy). ETS discloses a system, as modified above, where Kc/first key is generated based on the Ki/base key, message-specific data and RAND/data string (ETS, page 25) but lacks disclosure of the details of key-generating algorithm A8 (page 25, Fig. 4.1) and therefore lacks the first and second encryption key components hashing the base key, data strings and message-specific data to obtain a bias value. The only specification for algorithm A8 is that it is used to generate a key (ETS, page 49 §C.3). However, Hardy teaches a pseudo-random key can be generated by combining a document digest/message-specific data and at least one other secret value (such as Ki) using a hash, and inputting the result to a predefined pseudo-random key generator (col. 7 line 60 – col. 8 line 34). Hardy's system has the benefit of a reliably distinct key for each document/message signed (col. 7 lines 48-57). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to hash the

inputs to algorithm A8 (Ki, RAND, message-specific data) to obtain bias values to input to a key generator component configured to receive the bias value and generate the encryption keys based on the biased values. One of ordinary skill in the art would have been motivated to perform such a modification to obtain a reliably distinct key for each document/message signed, as taught by Hardy (col. 7 lines 48-57).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patents '766, '736, '591 & '928 are cited for teaching related knowledge in the art concerning one-time encryption keys, various encryption algorism using hashing, message-specific data and digital signatures appended to messages, respectively.

b. The non-patent literature are cited, but not relied upon, for teaching various, general techniques in securing mobile communications.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks

Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
March 17, 2004

3/18/04
NORMAN M. WRIGHT
PRIMARY EXAMINER